0. Skipping NSE scripting for Nmap is like bringing a spoon to a hacking knife fight!

Write a bash script that runs the default NSE scripts using `default` to perform various analyses and gather necessary information related to the target.

- Your script should accept a host as an arguments `$1`

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x07_nmap_post_port_scan_scripting]
└─⚑ sudo ./0-nmap_default.sh scanme.nmap.org
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-24 13:00 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 16.19 secon
```

The command:

```
nmap --script default $1
```

Explanation:

1. **`nmap`**:
    - Runs the Nmap network scanning tool.

2. `--script default`:
    - Specifies the **"default"** script category.
    - Scripts in the `default` category provide general-purpose functionality and safe operations.
    - These scripts are automatically included in scans like `-sC` or `-A`.

    Examples of scripts in the `default` category:

    - `ssl-cert`: Displays SSL/TLS certificate details.
    - `http-title`: Retrieves the title of HTTP services.
    - `ssh-hostkey`: Retrieves SSH host keys.
    - `default`: Scripts like version detection (`-sV`) and host discovery (`-Pn`) are included.
3. `$1`:
    - A **Bash positional parameter**.
    - Represents the **first argument** passed to the script or command.
    - In this case, `$1` is expected to be the target (e.g., an IP address, hostname, or network range).

How It Works:

- When the command is executed, Nmap runs all **default scripts** against the target specified in `$1`.
- Example usage:

  ```
  ./yourscript.sh 192.168.1.1
  ```

  Assuming `yourscript.sh` contains the command, `$1` will substitute `192.168.1.1`.

Example Output:

```
nmap --script default 192.168.1.1
```

Sample Output:

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 b3:5a:87:42:... (RSA)
|_  256 de:16:4e:1d:... (ECDSA)
80/tcp open  http
| http-title: Welcome to Apache Server
|_ssl-cert: Valid for 365 days, issued by Let's Encrypt
```

Practical Use Case:

Using `--script default` is an easy way to perform basic service enumeration while ensuring the scripts you run are **safe** and won't disrupt the network or services. Perfect for initial reconnaissance!